日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出　願　年　月　日
Date of Application:　　２００４年　４月１４日

出　願　番　号
Application Number:　　特願２００４－１１９２２５

パリ条約による外国への出願に用いる優先権の主張の基礎となる出願の国コードと出願番号
The country code and number of your priority application, to be used for filing abroad under the Paris Convention, is　　ＪＰ２００４－１１９２２５

出　願　人
Applicant(s):　　日本電信電話株式会社

２００５年　５月１１日

特許庁長官
Commissioner,
Japan Patent Office　　小川　洋

【書類名】　特許願
【整理番号】　NTTH157375
【提出日】　平成16年 4月14日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/08
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　唐澤　圭
【発明者】
　【住所又は居所】　東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
　【氏名】　松浦　克智
【特許出願人】
　【識別番号】　000004226
　【氏名又は名称】　日本電信電話株式会社
【代理人】
　【識別番号】　100066153
　【弁理士】
　【氏名又は名称】　草野　卓
【選任した代理人】
　【識別番号】　100100642
　【弁理士】
　【氏名又は名称】　稲垣　稔
【手数料の表示】
　【予納台帳番号】　002897
　【納付金額】　16,000円
【提出物件の目録】
　【物件名】　特許請求の範囲　1
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9806848

【書類名】特許請求の範囲
【請求項１】
インターネットと端末装置との間に接続される装置であって、
インターネットに接続された相手装置と前記端末装置との間のパケット通信に対し、前記相手装置との間で伝送されるパケットを暗号処理する鍵を表す鍵情報を前記相手装置と合意する必要があるか否かを、この鍵交換代理装置に受信されたパケットから判断するパケット判断手段と、
前記パケット判断手段が合意を必要とすると判断すると前記合意を行う鍵情報合意手段と、
前記鍵情報合意手段によって合意された鍵情報を前記端末装置に設定する鍵情報設定手段と、
を具備するパケット暗号処理の鍵交換代理装置。
【請求項２】
前記鍵情報は、前記パケットが伝送される通信路を確立するための暗号通信路情報に含まれ、前記合意は前記暗号通信路情報の合意であり、
前記鍵情報合意手段によって合意された暗号通信路情報を記憶する暗号通信路情報記憶手段を備え、
前記パケット判断手段は、鍵情報の合意を必要とすると判断すると前記受信パケットと対応する有効な暗号通信路情報が前記暗号通信路情報記憶手段にあるかを判断し、記憶手段にあればその暗号通信路情報中の鍵情報を前記鍵情報設定手段により前記端末装置に設定させ、なければ前記鍵情報合意手段に鍵情報の合意を実行させる手段であることを特徴とする請求項１に記載のパケット暗号処理の鍵交換代理装置。
【請求項３】
前記端末装置のアドレスを記憶するアドレス情報記憶手段を備え、
前記パケット判断手段は、前記鍵情報の合意を必要とすると判断し、かつ前記受信されたパケット内のアドレス情報が前記アドレス情報記憶手段に記憶されていれば前記鍵情報の合意を実行させるパケット判断手段であることを特徴とする請求項２に記載のパケット暗号処理の鍵交換代理装置。
【請求項４】
このパケット暗号処理の鍵交換代理装置に接続された端末装置を検知して、その端末装置からアドレス情報を取得し、その取得したアドレス情報を前記アドレス情報記憶手段に記憶するアドレス情報取得手段を備えたことを特徴とする請求項３に記載のパケット暗号処理の鍵交換代理装置。
【請求項５】
前記暗号通信路情報記憶手段は、前記暗号通信路情報中の少なくとも一部が記憶された、着脱可能な耐タンパ性デバイスを備えることを特徴とする請求項１～４のいずれかに記載のパケット暗号処理の鍵交換代理装置。
【請求項６】
前記暗号通信路情報記憶手段は前記暗号通信路情報中の少なくとも一部が変更可能な記憶媒体を備えることを特徴とする請求項１～４のいずれかに記載のパケット暗号処理の鍵交換代理装置。
【請求項７】
パケット暗号処理の鍵交換代理装置が、前記端末装置のネットワークインタフェイスデバイスに論理的に直接接続されていることを特徴とする請求項１～６のいずれかに記載のパケット暗号処理の鍵交換代理装置。
【請求項８】
前記インターネットと前記端末装置との間に接続され、ＩＰアドレスを持たないデバイスに前記パケット暗号処理の鍵交換代理装置が実装されていることを特徴とする請求項１～６のいずれかに記載のパケット暗号処理の鍵交換代理装置。
【請求項９】

受信されたパケットが鍵情報の合意を必要とするかをパケット判断手段により判断し、その判断結果が必要であればインターネットに接続された相手装置と端末装置との間のパケット通信に対し、前記相手装置との間で伝送されるパケットを暗号処理する鍵を表す鍵情報を鍵情報合意手段によって前記相手装置と合意し、

合意された鍵情報を鍵情報設定手段によって前記端末装置に設定し、

前記判断結果が必要でないならば前記受信されたパケットをバイパス又は廃棄することを特徴とするパケット暗号処理の鍵交換代理方法。

【請求項１０】

インターネットに接続された前記相手装置と前記端末装置の間のパケット通信における少なくともインターネット上のパケット通信に対し、暗号通信路の確立に用いる暗号通信路情報に前記鍵情報が含まれ、前記合意は前記暗号通信路情報の合意であり、

前記相手装置と前記合意をするとその合意した暗号通信情報を暗号通信路情報記憶手段に記憶し、

前記パケットに対する判断結果が必要であれば、前記受信パケットと対応する有効な暗号通信路情報が前記暗号通信路情報記憶手段にあるかを判断し、

その判断結果があるならばその暗号通信路情報中の鍵情報を前記鍵情報設定手段により前記端末装置に設定し、前記記憶手段に対する判断結果がないならば前記鍵情報合意手段により前記鍵情報の合意をすることを特徴とする請求項９に記載のパケット暗号処理の鍵交換代理方法。

【請求項１１】

前記パケットに対する判断結果が必要であれば、まず前記受信パケット内のアドレス情報がアドレス情報記憶手段に記憶されているかを判断し、その判断結果が記憶されているであれば、前記暗号通信路情報記憶手段にあるかの前記判断を行うことを特徴とする請求項１０記載のパケット暗号処理の鍵交換代理方法。

【請求項１２】

請求項１～８のいずれかに記載したパケット暗号処理の鍵交換代理装置としてコンピュータを機能させるためのプログラム。

【書類名】明細書
【発明の名称】パケット暗号処理の鍵交換代理装置、その方法及びプログラム
【技術分野】
【０００１】
この発明は、暗号化、復号化、署名、検証などの暗号処理を行う際に用いる鍵情報を相手装置と共有するための鍵交換機能を備えない端末装置とインターネットとの間に接続され、インターネットに接続された相手装置と前記端末装置間のパケット通信に対する、暗号処理する鍵を表す鍵情報を前記相手装置と合意する処理を行うパケット暗号処理の鍵交換代理装置、その方法及びプログラムに関するものである。
【背景技術】
【０００２】
従来、インターネット等の広域パケット通信ネットワークを介して暗号通信を行なうための規格として、インターネットの標準化組織であるＩＥＴＦ（Internet Engineering Task Force）により標準化され、フレーム構成、データの暗号化や改ざんチェックなどの規定に準拠したＩＰＳｅｃ（Security Architecture for Internet Protocol）が知られている。その他の暗号通信プロトコルの規格として、ＳＳＬ(Secure Sockets Layer)やＴＬＳ(Transport Layer Security)等がある。これらの規格は、事前に暗号および復号、署名および検証するための鍵、暗号および復号化アルゴリズム、署名および検証アルゴリズム、およびプロトコル等のＳＡ(Security Association)情報を合意しておく。このＳＡ情報の合意は、鍵交換プロトコルであるＩＫＥ(Internet Key Exchange)やハンドシェーク(Handshake)プロトコルに準拠して行われる。
【０００３】
これら鍵交換プロトコルを実行するには、ＳＡ情報を互いに合意する両者装置間で複数回の通信を行い、しかも計算処理量がかなり多く、これら装置に対し大きな負荷となる。従って、例えば家庭内の暗号処理通信機能を備える電子機器など小規模の端末装置にＳＡ情報合意機能を設けるとハードウェアおよびソフトウェア規模が大きくなり、大形化になりかつ価格も高くなる。このような点から前記小規模端末装置などにおけるＳＡ情報の合意一処理を端末装置に代って鍵支援代理装置で行うことが提案されている（例えば特許文献１参照）。
【０００４】
この特許文献１に示す鍵交換代理技術を図５を参照して簡単に説明する。
ネットワーク３１に接続され、鍵交換機能を備えない端末装置３２が、ネットワーク３１に接続され、鍵交換機能を備えた通信相手側端末装置３３とパケット暗号通信を行う場合、端末装置３２はまず通信相手側端末装置３３との暗号通信信号に用いる共通鍵の交換を、ネットワーク３１に接続された鍵交換代行サーバ３４に要求する。鍵交換代行サーバ３４はその要求に基づき、端末装置３２に代って通信相手側端末装置３３と鍵交換処理を行い、合意した共通鍵を端末装置３２に設定する。その後、端末装置３２はその合意した共通鍵を用いて通信相手側端末装置３３とパケット暗号通信を行う。
このような鍵交換代理処理をゲートウェイで行わせることが特許文献２に示されている。

【特許文献１】特開２００３－１７９５９２号公報
【特許文献２】特開２００３－２８９２９９号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
従来の鍵交換代理技術においては、ＳＡ情報のやり取りは鍵交換代理装置であり、通信パケットの送信先は端末装置である。従って、例えば図５に示した場合、端末装置３２はまず鍵交換代行サーバ３４と通信を行い、その後通信相手側端末装置３３との通信に切り替える必要があり、端末装置３２の利用者に手間をかけるという問題があった。
前述の従来技術では、インターネット等のネットワーク３１に端末装置３２、鍵交換代

サーバ３４と通信相手側端末装置３３がそれぞれ接続されており、端末装置３２と通信相手側端末装置３３との間で鍵交換処理を行うためには、端末装置３２と鍵交換代行サーバ３４が決められた情報の交換を行う必要がある。それゆえ端末装置３２や鍵交換代行サーバ３４は、ＣＰＵ、入出力インタフェイスの記憶部、入力部、出力部、通信部を備え、端末装置３２には、暗号データベースが接続されている。暗号データベースは、鍵交換代行サーバ３４、または通信相手側端末装置３３との通信の内容を暗号化するための鍵情報を記録している。また、鍵交換代行サーバ３４は、更にデータベースを有しており、このデータベースは、端末装置３２との通信の内容を暗号化するための鍵情報、通信相手側端末装置３３を認証する認証鍵に関する情報や端末装置３２へアクセスが許可された装置に関する情報等を記憶している。そのため端末装置３２は、通信相手側端末装置３３と鍵交換を行うまでに、鍵交換代行サーバ３４と鍵交換方法の決定処理、鍵生成処理や認証処理等の各種処理を行わなければならない。これらの処理が満足すると最終的に端末装置３２の暗号鍵データベースに鍵が設定される。以上のことから、鍵交換アルゴリズムの計算処理等の負荷の大きな処理が必要であり、その処理に多大な時間を要するという問題があった。また、ＳＡ情報のやり取りがパケット暗号処理の鍵交換代理装置である鍵交換サーバのために、通信相手側で鍵交換サーバと端末装置とを切り替えて通信を行う必要があり、通信相手に設定の手間をかけてしまうという問題があった。

【０００６】

この発明は、利用者に設定の手間をかけずに、鍵交換機能が実装されていない端末装置の鍵交換処理を代行することができるパケット暗号処理の鍵交換代理装置、その方法及びプログラムを提供することを目的とするものである。

【課題を解決するための手段】

【０００７】

この発明によるパケット暗号処理の鍵交換代理装置は、インターネットと端末装置との間に接続されて用いられ、パケット判断手段、鍵情報合意手段及び鍵情報設定手段を備え、インターネットに接続された相手装置と前記端末装置との間のパケット通信に対し、前記相手装置との間で伝送されるパケットを暗号処理する鍵を表す鍵情報の前記相手装置との合意をする必要があるか否かが、この鍵交換代理装置に受信されたパケットからパケット判断手段により判断され、この判断結果が必要とするならば前記合意が前記鍵情報合意手段により行われ、その合意された鍵情報が前記鍵情報決定手段により端末装置に設定される。

【発明の効果】

【０００８】

この発明のパケット暗号処理の鍵交換代理装置によれば、ネットワークと端末装置との間に接続されているから、鍵交換機能を備えない端末装置と、インターネットに接続された相手装置とのパケット暗号通信において、この鍵交換代理装置に受信されたパケットから鍵情報合意を必要とするか否かが判断され、その判断結果が必要とすれば鍵情報の合意が行われる。従って、鍵情報の合意要求と信号パケットとにより通信の相手、つまり送信先ＩＰアドレスの設定を切り替える必要がなく利用者に手間をかける煩雑さがない。

【発明を実施するための最良の形態】

【０００９】

以下、この発明の実施形態について、図面を参照して説明する。

図１は、この発明の一実施形態によるパケット暗号処理の鍵交換代理装置１を含むシステムの構成例を示すブロック図である。この発明は、ＩＰＳｅｃ、ＳＳＬまたはＴＳＬ等暗号通信プロトコルを利用する暗号通信におけるＳＡ情報の合意に適用することができるが、この実施形態においては、ＩＰＳｅｃによる暗号通信に適用するものとして説明する。さらにパケット暗号処理は暗号化処理、複合化処理、電子署名処理、その検証処理を表すが、この実施形態では暗号化処理および複合化処理について説明する。

パケット暗号処理の鍵交換代理装置１はインターネット２に接続され、インターネット２には相手装置３が接続される。パケット暗号処理の鍵交換代理装置１はパーソナルコン

ことのでき通信機能を備えた家庭内電気製品等の端末装置５に伝送路４を介して接続されている。

なお、相手装置３と端末装置５には、ＩＰＳｅｃ機能が実装されている。鍵交換機能は、相手装置３には実装されているが、端末装置５には実装されていない。

【００１０】

パケット暗号処理の鍵交換代理装置１は、ネットワーク２を介して接続された相手装置３等の装置と通信を行うネットワークインタフェイス９と、端末装置５と相手装置３との間で伝送されるパケットが鍵情報の合意を必要とするものであるか否かを判断するパケット判断手段１０を備えている。また、端末装置５と相手装置３との間で伝送されるパケットを暗号化および復号化する鍵情報を相手装置３と合意する鍵情報合意手段１１、その合意された鍵情報を端末装置５に設定する鍵情報設定手段１２、端末装置５なととの通信を行う端末インタフェイス１４を備えている。更に、この実施形態では端末装置５が前記パケットを伝送するための通信路を確立するのに必要な暗号通信路情報を記憶する暗号通信路情報記憶手段１３を備えた場合である。

本来の通信に先立ち相手装置３と端末装置５との間で双方が通信可能な手順の確認のネゴシエーション、つまり合意が鍵情報合意手段１１により行われ、その結果が暗号通信路情報として暗号通信路情報記憶手段１３に記憶される。

【００１１】

暗号通信路情報記憶手段１３は、例えば不揮発性の記憶媒体によって構成される。暗号通信路情報（以下、単に「ＳＡ（Security Association）情報」という）はＩＰＳｅｃが規定されているＲＦＣ（Request for Comments）2401に規定されたものであり、（１）ＳＡ情報を識別するための３２ビットの整数値で割り当てられて各パケット中に挿入され、パケット内の通信内容を示す識別番号（Security Parameter Index、ＳＰＩ）、（２）通信データ完全性を保証して転送し、またその検証を行うためのプロトコルであるＡＨ（Authentication Header）および通信データを秘匿して転送し、またその秘匿解除するためのプロトコルであるＥＳＰ（Encapsulating Security Payload）の何れかのプロトコルの情報を表すプロトコル情報、（３）暗号化や認証でそれぞれ使用される暗号アルゴリズムや鍵情報、（４）受信したパケットをＩＰヘッダを含めて暗号化して受信先へ転送するモードであるトンネルモードおよび、受信したパケット中のデータを暗号化しそれにＩＰヘッダを付加し、受信先に送るモードであるトランスポートモードの何れかのモードを表すモード情報、（５）ＩＰアドレス及びポート番号よりなる識別子、および（６）ＳＡ情報を変化させる時期などを示すＳＡ情報の生存時間等が含まれる。なお、ポート番号はインターネットで標準化されたサービスプロトコルに割り当てられた番号である。ＳＡ情報の各パラメータは、ＩＫＥ（Internet Key Exchange）等の鍵交換プロトコルによって通信相手との間で合意されるものであり、鍵情報合意手段１１は、端末装置５に代わってＳＡ情報の各パラメータを相手装置３と合意し、合意したパラメータが反映されたＳＡ情報を暗号通信路情報記憶手段１３に格納する。

【００１２】

鍵情報設定手段１２は、鍵情報合意手段１１によって合意されたＳＡ情報に含まれる鍵情報を端末装置５に設定するために、端末インタフェイス１４を介して鍵情報を端末装置５に送信する。端末装置５は、鍵情報設定手段１２によって送信された鍵情報に存在する鍵を使用して相手装置３との間で伝送されるパケットを暗号化や復号化する。

この実施形態ではパケット暗号処理の鍵交換代理装置１は、アドレス情報取得手段１５によって接続されている端末装置５を検知してそのアドレス情報（ＩＰアドレス）を取得し、その取得されたアドレス情報（ＩＰアドレス）は、アドレス情報記憶手段１６に記憶されるようにした場合である。なお、アドレス情報取得手段１５は、端末装置５からＩＰアドレスを取得する他に、例えば鍵情報合意手段１１によらず相互の話し合いなどで端末装置５に設定されているＳＡ情報を取得し、ＳＡ情報を暗号通信路情報記憶手段１３に格納することもできる。

【００１３】

更に、この実施形態では鍵情報合意手段１１は、相手装置３より鍵情報の交換要求があったとパケット判断手段１０で判断された場合、アドレス情報記憶手段１６に、鍵情報の交換要求先を示すＩＰアドレスが記憶されていると鍵情報の合意を行い、記憶されていない場合には鍵情報の合意を行わないようにした場合である。また、鍵情報合意手段１１は、端末装置５から相手装置３に通信の開始要求があったとパケット判断手段１０で判断された場合、アドレス情報記憶手段１６に、開始要求元示すＩＰアドレスが記憶されていると鍵情報の合意を行い、記憶されていない場合には鍵情報の合意を行わないようにした場合である。つまりパケット判断手段１０はこの鍵交換代理装置１に受信されたパケットのヘッダに示されている情報から鍵情報交換要求や通信開始要求など鍵情報の合意を必要とするものであるか否かを判断する。この判断結果が合意を必要とするならば直ちに鍵情報合意手段１６に鍵情報の合意を実行させてもよいが、この実施形態では、その受信されたパケットのヘッダに含まれている交換要求先又は開示要求先のＩＰアドレスがアドレス情報記憶手段１６に記憶されているかの判断を行い、その判断結果が記憶されているならば鍵情報合意手段１１に鍵情報の合意を実行させるようにした場合である。アドレス情報記憶手段１６にＩＰアドレスが記憶されているか否かの判断はパケット判断手段１０あるいは鍵情報合意手段１１により行う。

【００１４】

また、この実施形態では受信されたパケットより鍵情報の合意を必要とすると判断され、かつそのパケットのヘッダ中のＩＰアドレスがアドレス情報記憶手段１６に記憶されてあれば、暗号通信路情報記憶手段１３に対応する有効な暗号通信路情報が記憶されているかを判断し、有効な暗号通信路情報が記憶されてあれば、その鍵情報を鍵情報設定手段１２により前記端末装置５に設定し、記憶手段１３に記憶されていなければ前記鍵情報の合意を実行するようにした場合である。暗号通信路情報記憶手段１３に記憶されてあるか否かの判断はパケット判断手段１０又は鍵情報合意手段１１により行う。

なお、この実施形態ではパケット判断手段１０は、端末装置５と相手装置３との間で伝送されるパケットを相手側に送信するか、廃棄するかをアドレス情報記憶手段１６に記憶されたアドレス情報に基づいて判断し、判断結果に応じてパケットの処理を決定するようにした場合である。このため、アドレス情報、つまり相手装置３と端末装置５とのＩＰアドレスやポート番号の組み合わせと対応させてパケットの処理をアドレス情報記憶手段１６に記憶する。

【００１５】

図２は、アドレス情報記憶手段１６に記憶された情報の例を示す。図２において、１列目は、パケットの送信元を識別するための送信元識別情報中の送信元のＩＰアドレスを表し、２列目はパケットの送信先を識別するための送信先識別情報中の送信先のＩＰアドレス、３列目はパケットを伝送するための通信手順を表すプロトコル情報、４列目は送信元識別情報中の送信元のポート番号、５列目は送信先識別情報中の送信先のポート番号、および６列目はパケットをどのように処理するかを表す処理指示情報を表している。従って受信されたパケットについて、パケット判断手段１０がアドレス情報記憶手段１６に、あらかじめ記憶されているアドレス情報を参照し、その処理指示情報に応じて端末装置５に向けて送信されたパケットを、そのまま端末インタフェイス１４を介して送信するか、廃棄するかのパケットに対する処理を決定する。

【００１６】

図２中の１行目は、ＩＰアドレスがＩＰｖ４によって書かれており、送信元のＩＰアドレスが10.0.0.1/32、送信先のＩＰアドレスが10.0.0.*/24、（上位２４ビットが10.0.0.、下位８ビットが０～２４）および、プロトコル情報が信頼性を保証したコネクション形プロトコルであるtcp（Transmission Control Protocol）の場合には、送信元ポート番号及び送信先ポート番号が何であっても（ａｎｙ）、処理指示情報は相手装置３によって送信されたパケットをバイパスする。

また、２行目は、ＩＰアドレスがＩＰｖ６によって書かれており、送信元のＩＰアドレスが2001::1、送信先のＩＰアドレスが2001::2、プロトコル情報がパケットの紛失を許容

するコネクションレス形プロトコルであるudp（user datagram protocol）、および、送信元のポート番号と送信先のポート番号とが137の場合には、処理指示情報は相手装置３によって送信されたパケットを端末装置５にそのまま端末インタフェイス１４を介してバイパス送信する。

【００１７】

また、３行目は、送信元のＩＰアドレスが2001::1/128、送信先のＩＰアドレスが2001::2/128、プロトコル情報がＩＰ端末同士をコントロールするプロトコルであるicmp（Internet Control Message Protocol）、および、送信元のポート番号が135の場合には、処理指示情報は相手装置３によって送信されたパケットを廃棄する。なおこれらは例示であって、その識別情報やプロトコル情報と処理指示情報との間に関連はない。

図３は、パケット暗号処理の鍵交換代理装置１の相手装置３からのパケット受信動作を示すフローチャートである。パケット暗号処理の鍵交換代理装置１の相手装置３からのパケット受信動作は、ネットワーク２を介して相手装置３によって端末装置５に向けて送信されたパケットがネットワークインタフェイス９によって受信されたときにパケット暗号処理の鍵交換代理装置１は始まる。

【００１８】

まず、アドレス情報記憶手段１６に記憶されたアドレス情報に基づいて、ネットワークインタフェイス９によって受信されたパケットを端末装置５に端末インタフェイス１４を介して送信するか、パケットを廃棄するかパケット判断手段１０によって判断される（Ｓ１）。

ステップＳ１で、パケットを廃棄すると判断された場合には、ネットワークインタフェイス９によって受信されたパケットがパケット判断手段１０によって廃棄される（Ｓ２）。一方、パケットを端末装置５に端末インタフェイス１４を介して送信すると判断されたばあいには、パケットが鍵交換に関するものか否かがパケット判断手段１０によって判断される（Ｓ３）。

【００１９】

ステップＳ３で、パケットが鍵交換に関するものでないと判断された場合は、パケットが端末装置５に端末インタフェイス１４を介して送信される（Ｓ４）。一方、パケットが鍵交換に関するものであると判断された場合には、ステップＳ５で交換要求先ＩＰアドレスがアドレス情報記憶手段１６に記憶されているか判断され、記憶されていなければステップＳ２に移ってその受信パケットは廃棄される。

ステップＳ５で記憶されていると判断されると、ステップＳ６でその受信パケットに示されているＳＡ情報識別番号と同一でかつ有効なＳＡ情報が暗号通信路情報記憶手段１３に記憶されているかが判断され、記憶されていなければステップＳ７でＳＡ情報が鍵情報合意手段１１によって相手装置３と合意される。

【００２０】

ステップＳ７で、相手装置３と合意されたＳＡ情報は、ステップＳ８で暗号通信路情報記憶手段１３に記憶され、ステップＳ９で、ＳＡ情報に含まれる鍵情報は、鍵情報設定手段１２によって端末インタフェイス１４を介して端末装置５に送信される。ステップＳ６で有効なＳＡ情報が記憶されていると判断されると、ステップＳ９でその記憶されているＳＡ情報中の鍵情報を端末装置５へ送信する。なお、端末装置５と相手装置３との間で伝送されるパケットは、鍵情報設定手段１２によって送信された鍵情報に表される鍵を以って端末装置５において暗号化および復号化される。

【００２１】

図４は、パケット暗号処理の鍵交換代理装置１の端末装置５からのパケット受信動作を示すフローチャートである。この場合のパケット暗号処理の鍵交換代理装置１の動作は端末インタフェイス１４に端末装置５からのパケットが受信された時に始まる。

ステップＳ１１で端末インタフェイス１４によって受信されたパケットを相手装置３にネットワークインタフェイス９を介して送信するか、パケットを廃棄するかがアドレス情報記憶手段１６に記憶されたアドレスに基づいて、判断される。ステップＳ１１でパケッ

で廃棄すると判断された場合には、端末インタフェイス１４によって受信されたパケットがパケット判断手段１０によって廃棄される（Ｓ１２）。一方、パケットを相手装置３にネットワークインタフェイス９を介して送信すると判断された場合には、パケットが通信の開始要求を表すものか否かがパケット判断手段１０によって判断される（Ｓ１３）。

【００２２】

ステップＳ１３で、パケットが通信の開始要求を表すものでないと判断された場合には、パケットが相手装置３にネットワークインタフェイス９を介して送信される（Ｓ１４）。一方、パケットが通信の開始要求を表すものであると判断された場合には、ステップＳ１５で通信開始要求元ＩＰアドレスがアドレス情報記憶手段１６に記憶されているか判断され、記憶されていなければステップＳ１２に移ってその受信パケットは廃棄される。

ステップＳ１５で記憶されていると判断されると、ステップＳ１６でその受信パケットのヘッダに示されているＩＰアドレス、ポート番号などと対応するＳＡ情報が暗号通信路情報記憶手段１３に記憶されてあるか否かが判断され、記憶されていなければステップＳ１７でＳＡ情報が鍵情報合意手段１１によって相手装置３と合意される。

【００２３】

ステップＳ１７で、相手装置３と合意された情報は、暗号通信路情報記憶手段１３に記憶され（Ｓ１８）、ＳＡ情報に含まれる情報は、鍵情報設定手段１２によって端末インタフェイス１４を介して端末装置５に送信される（Ｓ１９）。ステップＳ１６でＳＡ情報が記憶されていると判断されると、ステップＳ１９でその記憶されているＳＡ情報中の鍵情報を端末装置５に送信する。なお、端末装置５と相手装置３との間で伝送されるパケットは、鍵情報設定手段１２によって送信された鍵情報に表される鍵を以って端末装置５において暗号化および復号化される。

【００２４】

以上で説明した、パケット暗号処理の鍵交換代理装置１の各構成要素は、上記で説明した動作をさせるように記述されたプログラムをプロセッサに実行させるようにしてもよい。すなわち、パケット判断手段１０、鍵情報合意手段１１、鍵情報設定手段１２およびアドレス情報取得手段１５は、上記プログラムを実行するコンピュータによって構成するようにしてもよい。この場合、コンピュータ内にこのパケット鍵交換代理プログラムをＣＤ－ＲＯＭ、磁気ディスク、半導体記憶装置などの記録媒体からインストール又は通信回線を通じてダウンロードしてそのプログラムをコンピュータに実行させればよい。

また、暗号通信路情報記憶手段１３およびアドレス情報記憶手段１６のうち少なくとも一方は、記憶した情報の少なくとも一部を、例えば暗号鍵情報、利用者名などを予定された（許された）以外の利用者が変更できないように、ＩＣカード、ＵＳＢ（Universal Serial Bus）キー、ＳＤ（Secure Digital）メモリカードなどの、耐タンパ性のある着脱可能なデバイスによって構成してもよい。

【００２５】

一方、暗号通信路情報記憶手段１３およびアドレス情報記憶手段１６のうち少なくとも一方は、インターネット２を介して認証された利用者であるならば、記憶した情報の少なくとも一部を変更できるようにしてもよい。つまり、例えば相手装置３と端末装置５との通信相手をダイナミックに変更し、これに伴いＩＰアドレスを変更する。この場合は、パケット暗号処理の鍵交換代理装置１には、ＩＰアドレスを割り当て、そのＩＰアドレスを用いてパケット暗号処理の鍵交換代理装置１とパケット通信を行って例えばそのアドレス情報記憶手段１６に記憶するアドレス情報に対する変更を行う。

【００２６】

上述において、パケット暗号処理の鍵交換代理装置は伝送路４を介して端末装置５と論理的に直接接続され、このパケット暗号処理の鍵交換代理装置１はＩＰ機能をもたないものであり、前記実施形態では受信したパケットが鍵交換を必要とするものか否かの判断をして、鍵交換を必要とする場合はパケット送信元及び送信先を変更することなく鍵合意を行って、その鍵情報を端末装置５に設定（送信）し、鍵交換を必要としないと判断された場合はパケットをそのまま転送するか、廃棄するものである。つまり鍵交換処理を行う場

ロと行わない場合ごとにより送信元ＩＰアドレスを変更する必要がなく、従来の、独立に設けられた鍵交換代行サーバやゲートウェイに設けられている、ＩＰ機能およびＩＰＳｅｃ機能と組み合わされた鍵交換代理機能とは異なる。

【００２７】

この発明のパケット暗号処理の鍵交換代理装置はインターネット２と端末装置５との間に接続されていればよく、例えば図１に破線で示すようにインターネット２と有線又は無線ＬＡＮ８を介して接続された各端末装置５に論理的に直接接続してよい。この場合は端末装置５にはＬＡＮ８との接続カード、つまりＩＰ機能及びＩＰＳｅｃ機能をもつ接続カードが装着されているからそのＬＡＮ接続カードなどのネットワークインタフェイスデバイスにパケット暗号処理の鍵交換代理装置１を搭載してもよい。

同様に図１中に破線で示すようにＬＡＮ８などに２ポートイーサネット（登録商標）ブリッジ６を介して端末装置５が接続されている場合のようにＩＰアドレスを持たないネットワーク間接続機器にこの実施形態のパケット暗号処理の鍵交換代理装置１を実装してもよい。つまりインターネットとゲートウェイを介し端末装置と接続されているＩＰアドレスを持たないデバイスにこの発明の鍵交換代理装置１を実装してもよい。さらにゲートウェイ７内にそのゲートウェイ機能と論理的に直列にこの発明の鍵交換代理装置１を実装してもよい。

【００２８】

この発明の鍵交換代理装置の最も簡単なものはパケット判断手段と鍵情報合意手段と鍵情報設定手段だけの機能をもっていればよく、つまりＩＰ機能及びＩＰＳｅｃ機能と切り離され、鍵交換を必要とするか否かの判断をし、必要な場合は鍵合意処理を行い、必要でない場合は単に通過させ又は廃棄するものである。従って単に端末装置のＩＰアドレスをパケットに設定すればよく端末装置のＩＰアドレスとパケット暗号処理の鍵交換代理装置のＩＰアドレスとの使い分けをして通信の切り替えをする必要がなく、相手装置の利用者に手間がかからない。

【００２９】

この発明において暗号処理とは前述したように、データを秘匿する、つまり暗号化する処理、その秘匿データの秘匿を解除する、つまり復号化する処理、電子署名などデータの完全性を保証する処理、その署名の検証などの完全性を確認する処理のいずれかであり、少なくともこれらのいずれかに必要とする鍵情報の合意にこの発明は適用される。従って相手装置３から受信したパケットに対してのみこの発明を適用してもよく、逆に端末装置５から受信したパケットに対してのみこの発明を適用してもよい。図１に示した鍵交換代理装置１において暗号通信路情報記憶手段１３、アドレス情報取得手段１５、アドレス情報記憶手段１６を省略してもよい。この場合は図３において、ステップＳ５、Ｓ６及びＳ８は省略され、図３中に破線４０で示すようにステップＳ３で鍵交換に関するものと判断されるとステップＳ７に直ちに移り、ステップＳ７の後、ステップＳ９に直ちに移る。また図４において、ステップＳ１５、Ｓ１６及びＳ１８は省略され、図４中に破線５０で示すようにステップＳ１３で通信開始要求と判断されるとステップＳ１７に直ちに移り、ステップＳ１７の後にステップＳ１９に直ちに移る。

【００３０】

また図１に示した鍵交換代理装置１において、アドレス情報取得手段１５及びアドレス情報記憶手段１６を省略してもよい。この場合は図３においてステップＳ５が省略され、図３中に破線４１で示すようにステップＳ３で鍵交換に関するものと判断されると、直ちにステップＳ６に移る。また図４においてステップＳ１５が省略され、図４中に破線５１で示すように、ステップＳ１３で通信開始要求と判断されるとステップＳ１６に直ちに移る。

暗号通信路情報記憶手段１３を設ける場合は、これに記憶されている有効なＳＡ情報を利用でき、それだけこの鍵交換代理装置１における処理量が少なくなる。またアドレス情報記憶手段１６を設ける場合も、もともと通信することができない相手装置３と端末装置５間について無駄な鍵情報の合意を行わないで済む利点がある。

【００３１】

アドレス情報取得手段１５を省略すると、暗号通信路情報記憶手段１３及びアドレス情報記憶手段１６に対するＳＡ情報の一部及びアドレス情報の記憶を人手により行うことになるが、アドレス情報取得手段１５を設ける場合は、パケット暗号処理の鍵交換代理装置１がこれに接続されている端末装置５のＩＰアドレスやサービス等の機器情報を収集し、収集した機器情報に基づいてポート番号やプロトコルの種別などのＩＰアドレスを生成して、記憶手段１３又は／及び１６に記憶する情報の一部を記憶することができ、利用者による入力を支援することができる。

【００３２】

端末装置５は例えば、空調機、照明器具、洗濯機、電話機、電子レンジ、テレビジョン受像機、パーソナルコンピュータなどの家庭内電気機器、事務用電気機器などその他あらゆる電気機器であって、ＩＰ機能及びＩＰＳｅｃ機能を備えるものである。ＬＡＮ８は無線ＬＡＮ，有線ＬＡＮでもよく、用途的に云えばホームネットワーク、企業内ネットワーク、学校内ネットワーク、地域ネットワーク、病院内ネットワークなどである。

鍵交換代理装置１に複数の端末装置５が接続され、これら端末装置５が同じ相手装置３とパケット暗号通信を行う場合は、鍵情報合意手段１１は、相手装置３とパケット暗号通信を行う場合は、鍵情報合意手段１１は、相手装置３とその間に、情報の改ざんや漏洩が防止された安全な通信路を確立して、各端末装置５と相手装置３との鍵情報の合意をそれぞれ個々に行う。

【図面の簡単な説明】

【００３３】

【図１】この発明の一実施形態によるパケット暗号処理の鍵交換代理装置を含むシステム構成例を示すブロック図。

【図２】この発明の一実施形態におけるアドレス情報記憶手段１６に記憶された情報の例を示す図。

【図３】この発明の一実施形態によるパケット暗号処理の鍵交換代理方法における相手装置から受信したパケットに対する処理手順の例を示すフローチャート。

【図４】この発明の一実施形態によるパケット暗号処理の鍵交換代理方法における端末装置から受信したパケットに対する処理手順の例を示すフローチャート。

【図５】従来の鍵交換代行サーバを含むシステムを示す図。

【図面】

【図１】

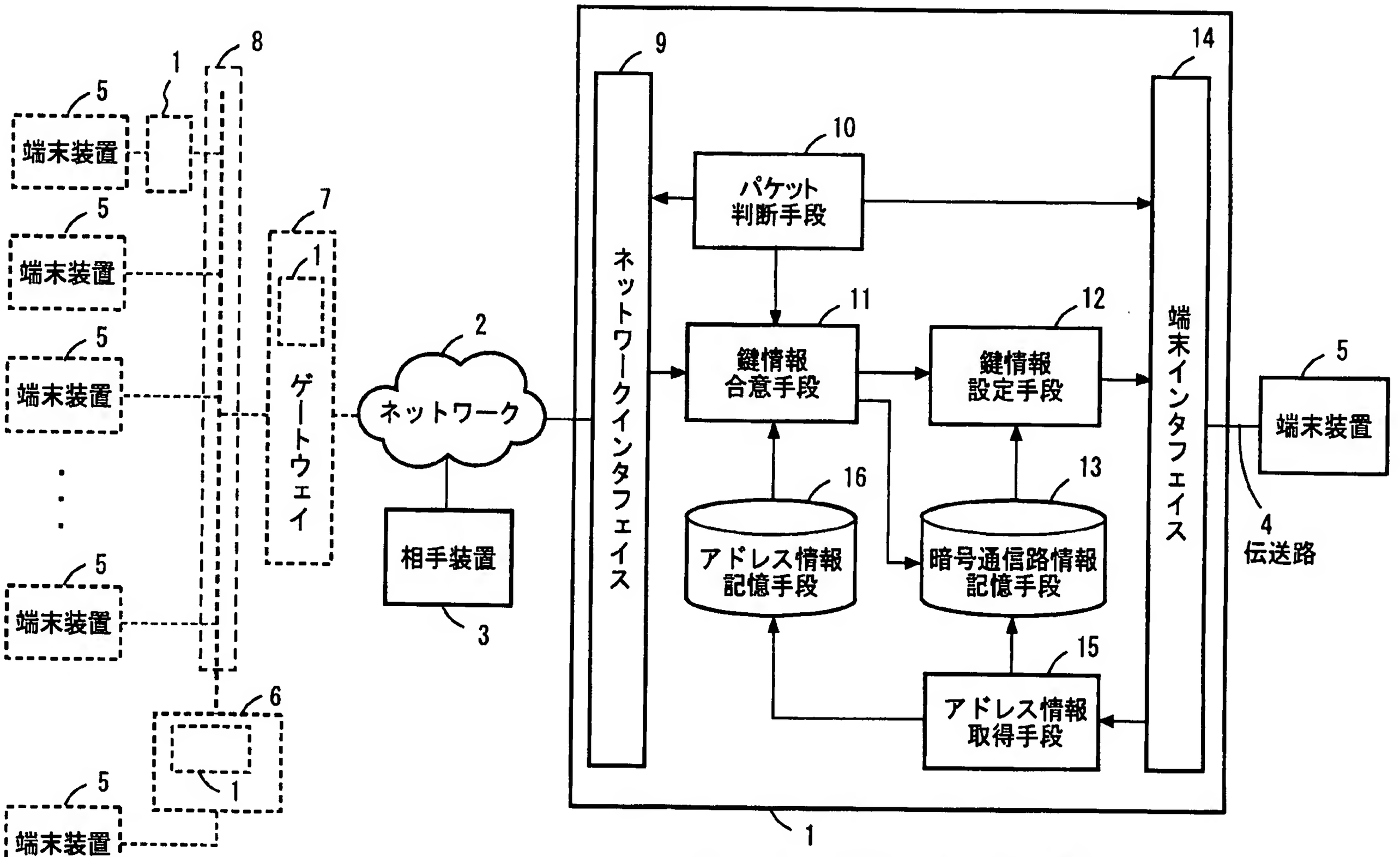
端末装置
端末装置
端末装置
端末装置
端末装置
端末装置
ゲートウェイ
ネットワーク
相手装置
ネットワークインタフェイス
パケット判断手段
鍵情報合意手段
鍵情報設定手段
端末インタフェイス
端末装置
アドレス情報記憶手段
暗号通信路情報記憶手段
アドレス情報取得手段
伝送路
パケット暗号処理の鍵交換代理装置

図1

送信元IPｱﾄﾞﾚｽ	送信先IPｱﾄﾞﾚｽ	ﾌﾟﾛﾄｺﾙ	送信元ﾎﾟｰﾄ番号	送信先ﾎﾟｰﾄ番号	処理指示
10.0.0.1/32	10.0.0.*/24	tcp	any	any	バイパス
2001::1	2001::2	udp	137	137	バイパス
2001::1/128	2001::2/128	icmp	135	N/A	廃棄

図2

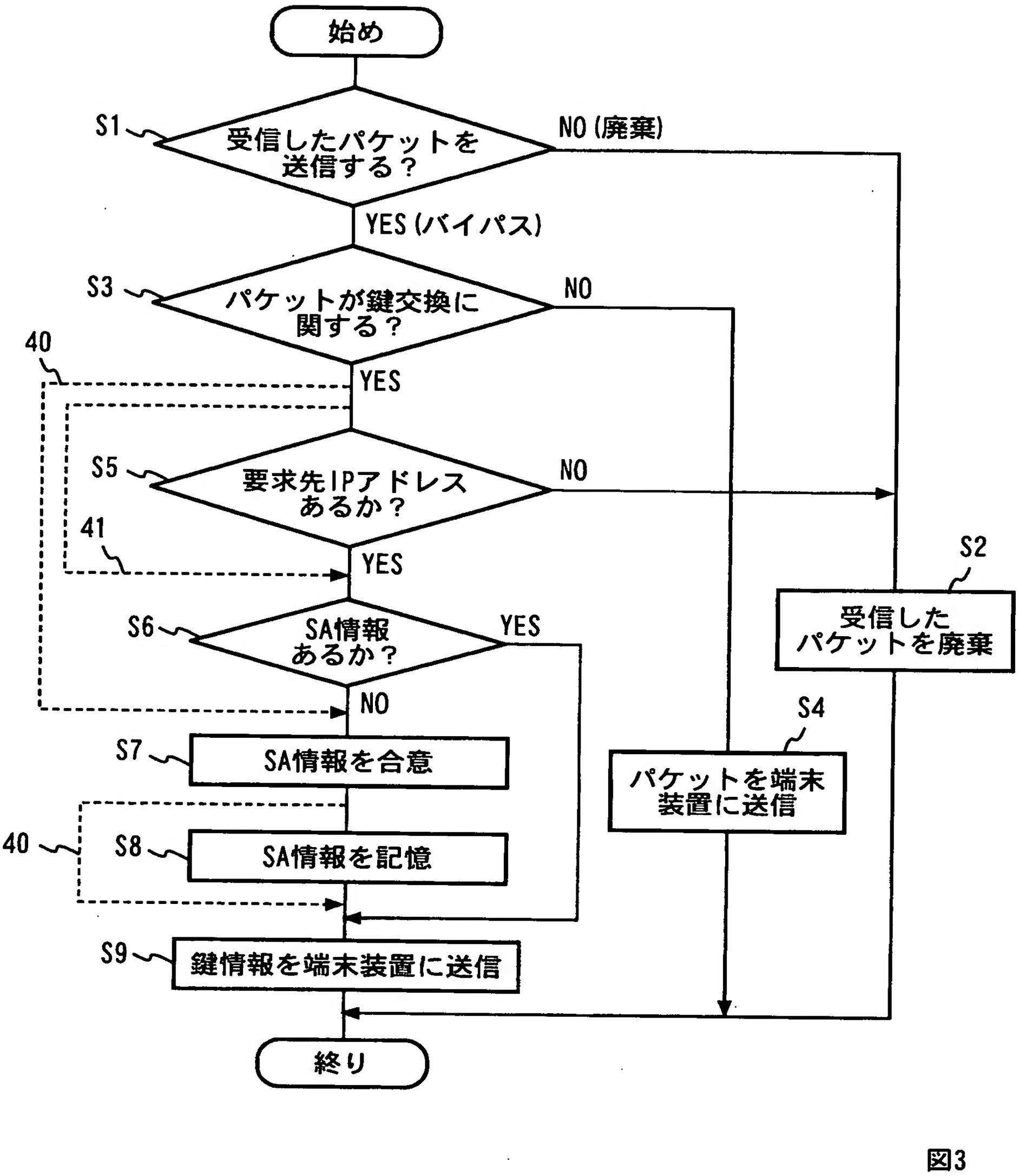
始め
S1
受信したパケットを送信する？
NO (廃棄)
YES (バイパス)
S3
パケットが鍵交換に関する？
NO
40
YES
S5
要求先IPアドレスあるか？
NO
41
YES
S6
SA情報あるか？
YES
NO
S7
SA情報を合意
40
S8
SA情報を記憶
S9
鍵情報を端末装置に送信
終り
S2
受信したパケットを廃棄
S4
パケットを端末装置に送信

図3

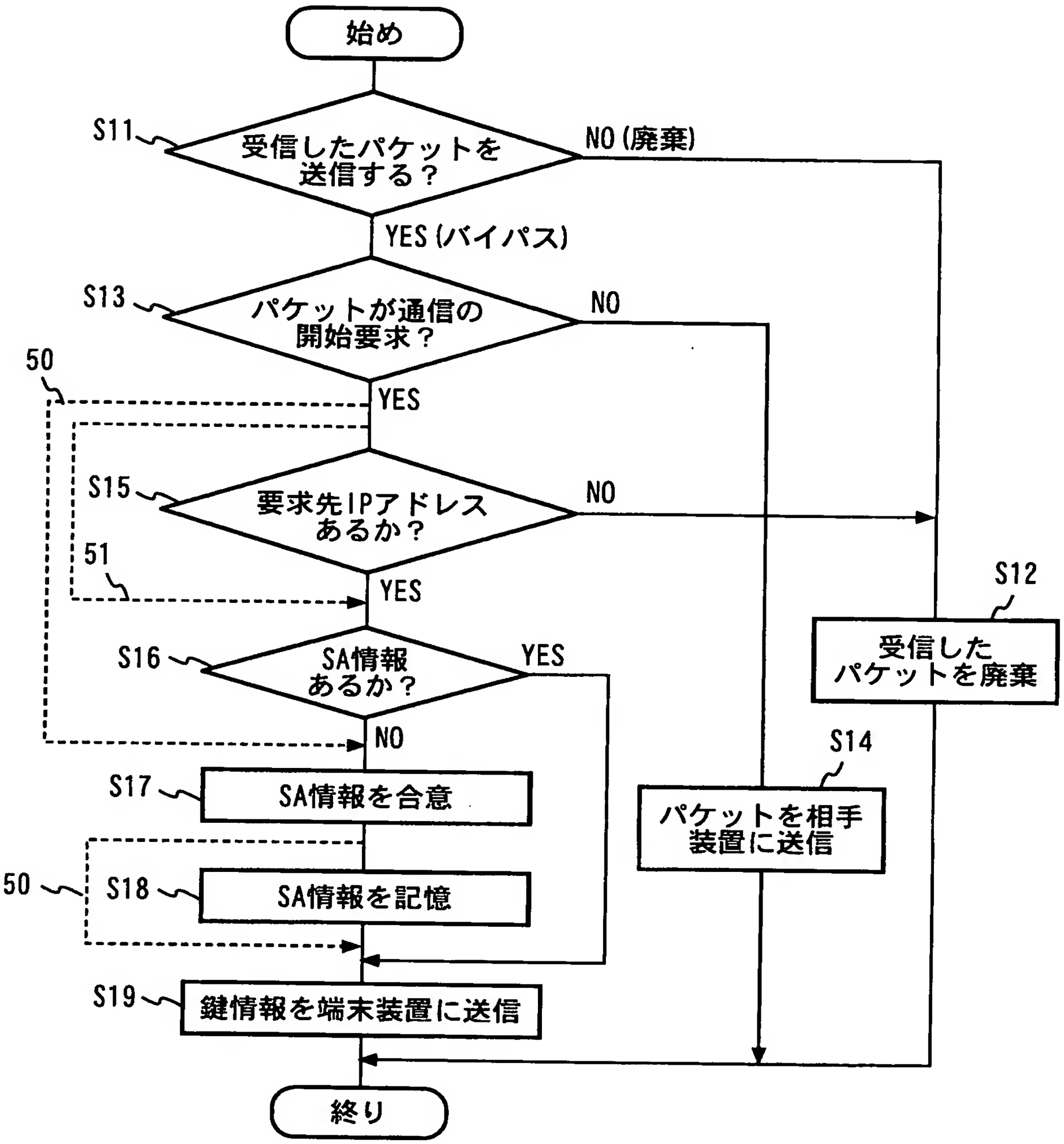
始め
S11
受信したパケットを送信する？
NO (廃棄)
YES (バイパス)
S13
パケットが通信の開始要求？
NO
50
YES
S15
要求先IPアドレスあるか？
NO
51
YES
S12
受信したパケットを廃棄
S16
SA情報あるか？
YES
NO
S14
パケットを相手装置に送信
S17
SA情報を合意
50
S18
SA情報を記憶
S19
鍵情報を端末装置に送信
終り

図4

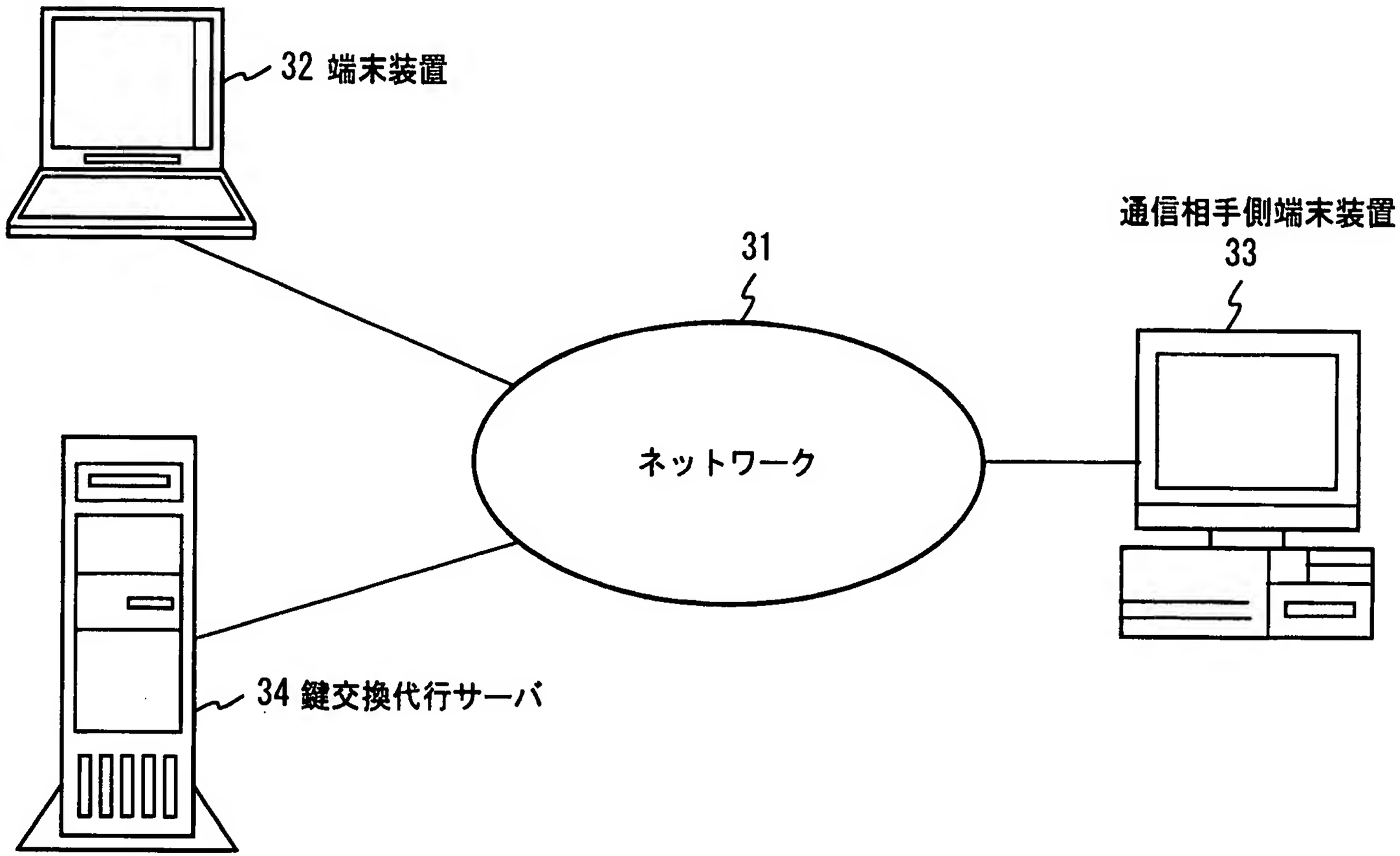

図5

【書類名】 要約書

【要約】

【課題】　鍵交換処理機能がない端末５に対し、鍵交換処理の代理をし、鍵交換代理要求と本来の暗号通信との通信切り替えの手間を利用者にかけない。

【解決手段】　インターネット２に接続された相手装置３からパケットが受信されると、そのパケットが鍵交換に関するものか否かをパケット判断手段１０により判断し、鍵交換に関するものであればパケット送信先の端末５と相手装置３との間の鍵情報の合意を鍵情報合意手段１１で行い、その合意された鍵情報を鍵情報設定手段１２によって端末５に設定し、受信したパケットが鍵交換に関するものでなければそのパケットを端末５へ転送する。

【選択図】　図１

０００００４２２６
19990715
住所変更
５９１０２９２８６

東京都千代田区大手町二丁目３番１号
日本電信電話株式会社

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/006624

International filing date: 04 April 2005 (04.04.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-119225
Filing date: 14 April 2004 (14.04.2004)

Date of receipt at the International Bureau: 26 May 2005 (26.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)